AMENDMENT AND PRESENTATION OF CLAIMS

Please replace all prior claims in the present application with the following claims.

1-50. (Canceled)

51. (New) A network access system comprising:

at least one programmable access device, including first and second network interfaces through which packets are communicated with a first network and a second network respectively, wherein the at least one programmable access device comprises a forwarding table for routing packets between the first and second network interfaces, and a packet header filter for identifying messages received at one of the network interfaces on which policy-based services are to be implemented and for generating the identified messages via a message interface;

an external processor, separate and distinct from the at least one programmable access device, and configured to implement policy-based services by receiving and processing the identified messages from the message interface, wherein the external processor comprises one or more service controllers for controlling functions for a respective type of service, at least one programmable access device controller for configuring the forwarding table, the packet header filter, and at least one other function of an associated programmable access device, and a message processor for the associated programmable access device for communicating messages to/from the message interface of the associated programmable access device; and

an access router separate and distinct from both the external processor and the at least one programmable access device, wherein the access router is configured to route packets

from the first network interface to the second network interface based on the forwarding table in the at least one programmable access device.

52. (New) The network access system of claim 51, wherein messages not identified by the packet head filter are passed to a policer within the associated programmable access device for discarding packets determined as nonconforming to a traffic parameter.

53. (New) The network access system of claim 52, wherein a second packet header filter, different from the first packet header filter, is coupled to the second network interface, wherein the second packet header filter identifies messages received from the second network interface, on which policy-based services are to be implemented, wherein the second packet header filter passes the identified messages to the external processor via the message interface and passes all other messages received from the second network interface to the policer.

54. (New) The network access system of claim 51, wherein the at least one other function of an associated programmable access device comprises dynamic allocation of resources to one of a customer interface, a packet flow, a class, and a multicast group.

55. (New) The network access system of claim 53, wherein the policer polices a packet stream by applying one or more token or leaky bucket algorithms to determine whether the packet stream conforms to the traffic parameter.

56. (New) The network access system of claim 53, wherein the associated programmable access device further comprises at least a usage monitor that monitors at least one traffic type.

57. (New) The network access system of Claim 56, wherein the usage monitor has an associated threshold that when exceeded generates a reporting event for the usage monitor.

58. (New) The network access system of Claim 57, and further comprising a reporting interface that communicates the reporting event to the external processor.

59. (New) The network access system of Claim 58, wherein the associated threshold comprises a session activity level threshold.

60. (New) The network access system of Claim 56, and further comprising a fault monitor.

61. (New) A method of packet handling in a network access system, said method comprising:

in response to receiving a series of packets at a first network interface of a programmable access device associated with an external processor, filtering the series of packets by a packet header filter at the programmable access device to identify messages upon which policy-based services are to be implemented;

passing identified messages to the external processor for implementation of the policy-based services by the external processor, wherein the external processor controls functions for a respective type of service, configures a forwarding table, a packet header filter, and at least one other function of the associated programmable access device, and communicates messages to/from the message interface of the associated programmable access device;

for messages that are not identified, routing packets, via an access router, by reference to the forwarding table in the associated programmable access device and outputting the routed packets at a second network interface of the associated programmable access device; and

programming the packet header filter and the forwarding table of the associated programmable access device by the external processor through a control interface of the associated programmable access device.

62. (New) The method of claim 61, wherein messages not identified by the packet head filter are passed to the associated programmable access device for discarding packets determined as nonconforming to a traffic parameter.

63. (New) The method of claim 62, wherein a second packet header filter, different from the first packet header filter, is coupled to the second network interface, wherein the second packet header filter identifies messages received from the second network interface, on which policy-based services are to be implemented, wherein the second packet header filter passes the identified messages to the external processor via the message interface and passes all other messages received from the second network interface to a policer within the associated programmable access device.

64. (New) The method of claim 61, wherein the at least one other function of the associated programmable access device comprises dynamic allocation of resources to one of a customer interface, a packet flow, a class, and a multicast group.

65. (New) The method of claim 63, wherein one or more token or leaky bucket algorithms is applied to a packet stream to determine whether the packet stream conforms to the traffic parameter.

66. (New) The method of claim 63, wherein the associated programmable access device monitors at least one traffic type.

67. (New) The method of Claim 66, wherein the monitoring of the at least one traffic type employs an associated threshold that when exceeded generates a reporting event.

68. (New) The method of Claim 67, wherein the reporting event is communicated to the external processor.

69. (New) The method of Claim 68, wherein the associated threshold comprises a session activity level threshold.

70. (New) The method of Claim 66, wherein the monitoring is performed by a fault monitor.